MICROSENS

24 Port Gigabit Ethernet PoE Switch

User Manual

MS400830M

Release 1.44
April, 2014

Table of Contents

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.
- In case of connection to an outdoor device with cable, you need to add an outdoor arrester between this device and the switch (see Fig. 1)

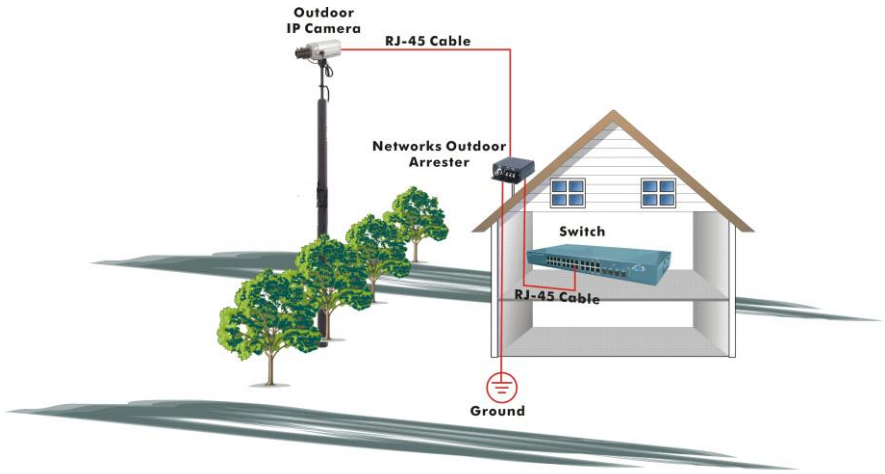


Fig. 1 Addition of an arrester between outdoor device and this switch

Electronic Emission Notices

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard **EN55022/EN61000-3** and the Generic European Immunity Standard EN55024.

EMC:

EN55022 (2003) / CISPR-2 (2002)	class A
IEC61000-4-2 (2001)	4 kV CD, 8 kV
IEC61000-4-3 (2003)	3V/m
IEC61000-4-4 (2001)	1 kV (power line); 2 kV (signal line)

Warning:

- It is expressly prohibited to open the switch! Damage caused by opening will be charged.
- Do not place product at outdoor or sandstorm.
- Before installation, please make sure input power supply and product specifications are compatible to each other.

1. Introduction

1-1. Overview of 24 Port Gigabit Ethernet Switch

The 24 Port Gigabit Ethernet Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit and Fast Ethernet specifications. The switch has 20 10/100/1000Mbps TP ports and 4 Gigabit TP/SFP combo ports. All TP ports support IEEE802.3af (PoE 15.4W) and IEEE802.3at (PoE+ 30W) standard. The device supports http interface for switch management. The network administrator can logon the switch to monitor, configure and control each port's activity. In addition, the switch implements QoS (Quality of Service), VLAN and Trunking. It is suitable for office application.

In this switch, Port 21, 22, 23, 24 include two types of media – TP ports and SFP slots; the TP ports support 10/100/1000Base-TX while the SFP fiber ports support Gigabit Ethernet with auto-detected function.

10/100/1000Mbps TP is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit and Fast Ethernet specifications. The Gigabit Ethernet SFP ports fully comply with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceivers are also available. They are designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

• Key Features

QoS:

The switch offers powerful QoS function. This function supports 802.1p VLAN tag priority and DSCP on Layer 3 of network frame work.

RSTP / STP:

Rapid Spanning Tree according to 802.1w. This function allows the use of redundant links. The previous STP standard according to 802.1d is also selectable.

VLAN:

IEEE802.1Q Tag VLAN. Up to 24 active VLANs (VLAN ID range: 1~4094).

Port Trunking:

Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting.

PoE:

24 PoE ports allow power to be supplied to end devices, such as Wireless Access Points or VoIP Phones, directly through the existing LAN cables, eliminating costs for additional AC wiring and reducing installation cost. It is compliant with IEEE802.3af standard. It provides the endpoint with 48VDC power through RJ-45 pin 1, 2, 3, 6. Totally 370 watts for PoE powering are provided (Up to 15.4 W for 24 ports).

1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

- 24 Port Gigabit Ethernet Switch with PoE and WEB management
- Mounting Accessory (for 19” Rack Shelf)
- This User's Manual in CD-ROM
- AC Power Cord

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

1-3. Features

This switch provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

Hardware

- 20 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports
- 4 dual media ports (10/100/1000Mbps TP or 1000Mbps SFP with auto sense)
- 512KB on-chip frame buffer
- 370 watts for PoE
- Rack mounting option
- Jumbo frame support 9KB
- Power Saving with "ActiPHY Power Management" and "Perfect Reach Power Management" techniques.
- Programmable classifier for QoS (Layer 2 / Layer 3)
- 8k MAC address and support and 24 different VLAN IDs out of 1~4094
- Broadcast Storm Control
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs: System, Power; TP Port1-24: LINK/ACT, PoE, 10/100/1000Mbps; SFP Port 21,22,23,24: (LINK/ACT)

Management

- Supports concisely the status of port and easily port configuration
- Supports per port traffic monitoring counters
- Supports port mirror function
- Supports the static trunk function
- Supports RSTP according to 802.1w and STP (802.1d)
- Supports 802.1Q VLAN
- Supports user management and limits one user to login
- Maximal packet length can be up to 9600 bytes for jumbo frame application
- Supports Broadcasting Suppression to avoid network suspended or crashed
- Supports to send the trap event while monitored events happened
- Supports default configuration which can be restored to overwrite the current configuration which is working on via Web UI and reset button of the switch
- Supports on-line plug/unplug SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 3.
- Built-in web-based management instead of using CLI interface, providing a more convenient GUI for the user

1-4. View of 24 Port Gigabit Ethernet Switch

Fig. 1-1 Full View of 24 Port Gigabit Ethernet Switch: MS400830M

1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs)

There are 20 TP Ports (10/100/1000Base-T) and 4 dual media ports (UTP/SFP) on the front side. LED display area, locating on the left side of the panel, contains a System LED, which indicates the power status and 24 port LEDs working status of the switch. Below the system LED there are 3 LEDs (Link/Act, Speed, PoE) which indicate the LED mode. The LED mode can be change by pressing the Mode button. Warning! Pressing the Mode button for around 5 seconds will cause a Factory Default Reset.

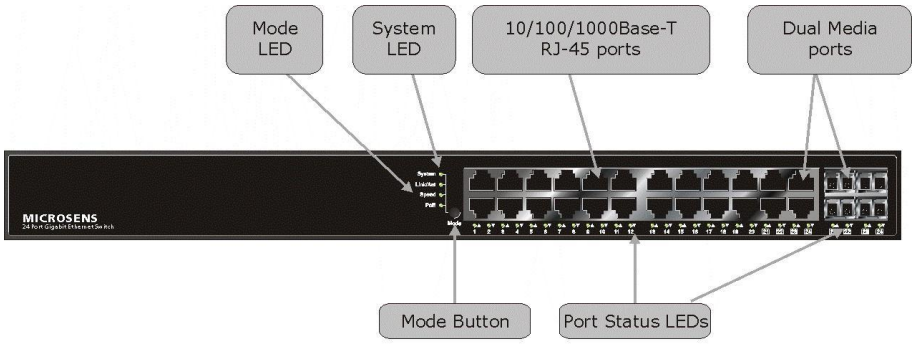


Fig. 1-2 Front view

● LED Indicators

LED	Color	Function
System/Mode LED		
System	Green	Lit when +3.3V power is coming up
Link/Act	Green	Lit when Link/Act LED mode is active
Speed	Green	Lit when Speed LED mode is active
PoE	Green	Lit when PoE LED mode is active
10/100/1000Ethernet TP Port 1 to 24 LED		
Link/Act	Green	Lit when connection with remote device is good Blinks when any traffic is present
Speed	Green/ Yellow/ Off	Lit Green when TP link on 1000Mbps speed Lit Yellow when TP link on 10/100Mbps speed Off when no link occur
PoE	Green	Lit when PoE Power is active
1000SX/LX Gigabit Fiber Port 21 - 24 LED		
LINK/ACT	Green	Lit when SFP connection with remote device is good Blinks when any traffic is present
Speed	Green/ Yellow/ Off	Lit Green when SFP link on 1000Mbps speed Lit Yellow when SFP link on 100Mbps speed Off when no link occur

Table1-1

1-4-2. User Interfaces on the Rear Panel

Fig. 1-3 Rear view

1-5. View of Optional Modules

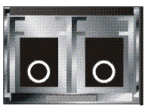


Fig. 1-4 Front view of standard SFP transceiver

2. Installation

2-1. Starting up 24 Port Gigabit Ethernet Switch

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2-1-1. Hardware and Cable Installation

At the beginning, please do first:

⇒ Wear a grounding device to avoid the damage from electrostatic discharge

⇒ Be sure that power switch is OFF before you insert the power cord to power source

- **Installing optional SFP fiber transceivers to the 24 Port Gigabit Ethernet PoE Switch**

  Note: If you have no modules, please skip this section.

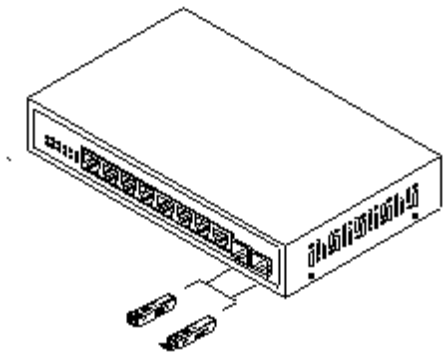


Fig. 2-1 Installation of optional SFP transceiver

- **Connecting the SFP Module to the Chassis:**

The optional SFP modules are hot swappable, so you can plug or unplug them before or after powering on.

1. Verify that the SFP module is the right model and conforms to

   the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into slot(s)
5. Have the power ON after the above procedures are done

• TP Port and Cable Installation

⇒ In the switch, TP ports support MDI/MDI-X auto-crossover, so both types of cable, straight-through and crossed-over can be used. It means you do not have to tell from them, just plug it.

⇒ Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device such as a workstation or a server.

⇒ Repeat the above steps, as needed, for each RJ-45 port to be connected to a 10/100/1000Base-T device.

Now, you can start having the switch in operation.

• Power On

The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection plugged into the switch or not when power on, even modules as well. After the power is on, all LED indicators will light up and then all off except the power LED still keeps on. This represents a reset of the system.

• Firmware Loading

After resetting, the boot loader will load the firmware into the memory. It will take about 30 seconds, after that, the switch will flash all the LED once and automatically performs self-test and is in ready state.

2-1-2. Cabling Requirements

To help ensure a successful installation and keep the network performance good, please take a care on the cabling requirement. Cables with worse specification will render the LAN to work poorly.

2-1-2-1. Cabling Requirements for TP Ports

⇒ For Fast Ethernet TP network connection
  — The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters.

⇒ Gigabit Ethernet TP network connection
  — The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters. Cat. 5e is recommended.

2-1-2-2. Cabling Requirements for 1000Base-SX/LX SFP Modules

It is more complex and comprehensive contrast to TP cabling in the fiber media. Basically, there are two categories of fiber, Multimode (MM) and Single Mode (SM). From the viewpoint of connector type, there mainly are LC (standard) and BIDI SC.

The following table lists the types of fiber that we support and those else not listed here are available upon request.

IEEE 802.3z Gigabit Ether-net 1000SX 850nm	Multimode Fiber Cable and Modal Bandwidth			
	Multi-mode 62.5/125μm		Multi-mode 50/125μm	
	Modal Bandwidth	Distance	Modal Bandwidth	Distance
	160MHz-Km	220m	400MHz-Km	500m
	200MHz-Km	275m	500MHz-Km	550m
1000Base-LX/LHX/XD/ZX	Single-mode Fiber 9/125μm			
	Wavelength and distance depend on used SFP module			

Table2-1

2-1-2-3. Switch Cascading in Topology

● Takes the Delay Time into Account

Theoretically, the switch partitions the collision domain for each port in switch cascading that you may up-link the switches unlimitedly. In practice, the network extension (cascading levels & overall diameter) must follow the constraint of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire	11.12/m	Cat.5 TP Wire	1.12/m	Fiber Cable	1.0/m
Fiber Cable	10.10/m	TP to fiber Converter: 56			
Bit Time unit: 1ns (1sec./1000 M bit)		Bit Time unit: 0.01μs (1sec./100 Mbit)			

Table 2-2

Sum up all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

• Typical Network Topology in Deployment

A hierarchical network with minimum levels of switch may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. Server/Host is recommended to connect to the Level 1 switch. This is general if no VLAN or other special requirements are applied.
Case1: All switch ports are in the same local area network.
Every port can access each other (See Fig. 2-2) *

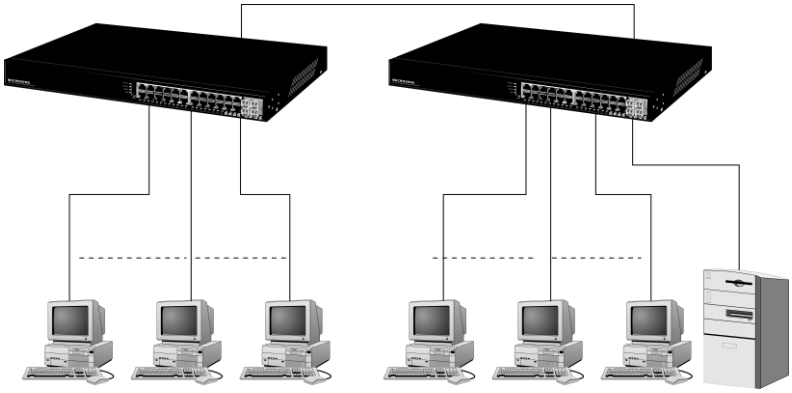


Fig. 2-2 No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded in the same VLAN area.

Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

Case2a: Port-based VLAN (See Fig.2-3).

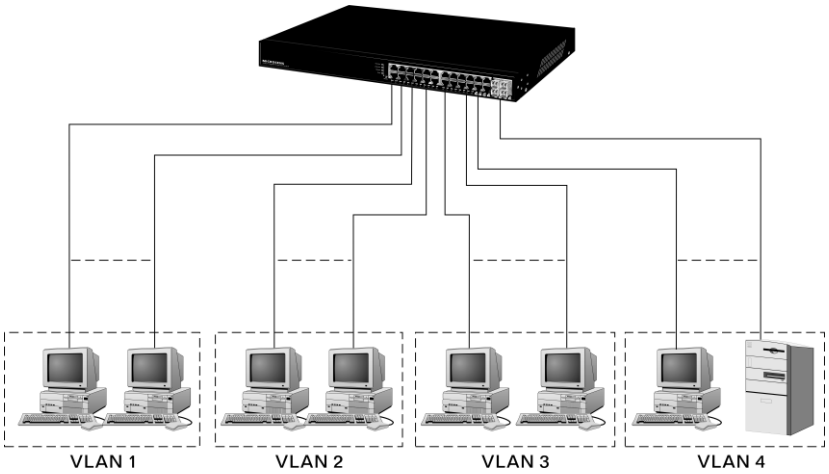


Fig. 2-3 Port-based VLAN Diagram

1. The same VLAN members could not be in different switches.
2. Every VLAN members could not access VLAN members each other.
3. The switch manager has to assign different names for each VLAN groups at one switch.

Case 2b: Port-based VLAN (See Fig.2-4).

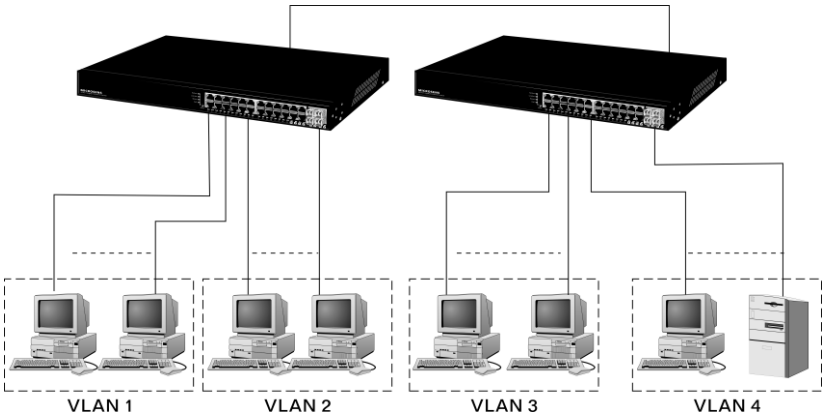


Fig. 2-4 Port-based VLAN Diagram

1. VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
3. VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-5)

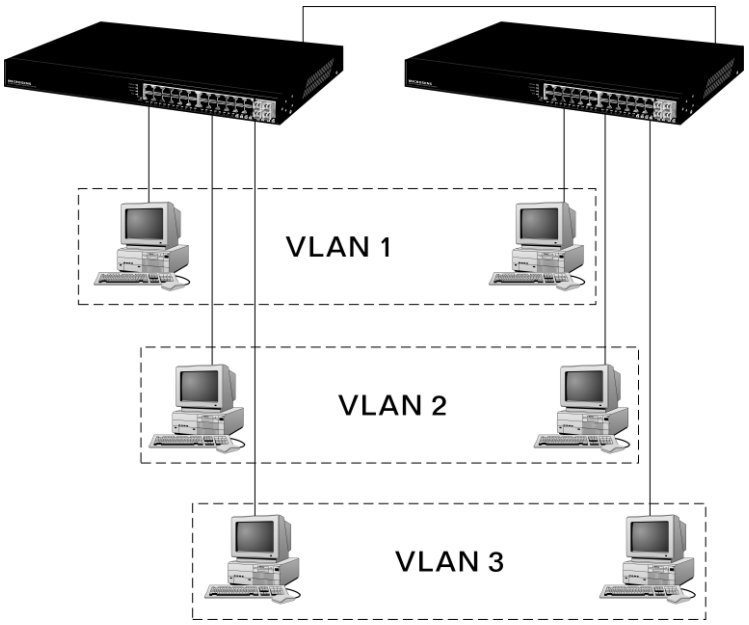


Fig. 2-5 Attribute-based VLAN Diagram

2-1-3. Configuring the Management Agent

In the way of web, user is allowed to startup the switch management function. Users can use any one of them to monitor and configure the switch. You can touch them through the following procedures described in section 2-1-3-1.

2-1-3-1. Configuring Management Agent

For complete configuration and monitoring a web browser has to be used. Basic information can be obtained using a SNMP manager. Web-based UI for the switch is an interface in a highly friendly way.

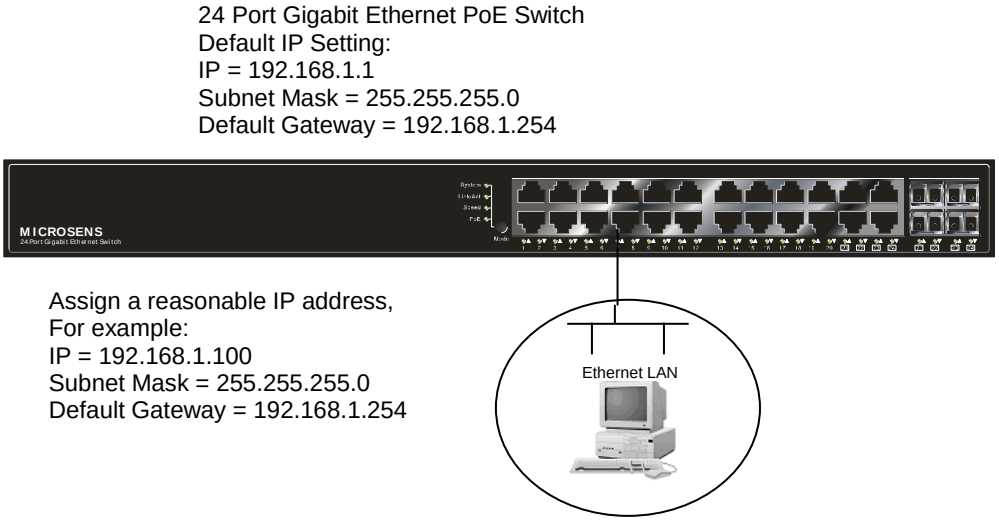


Fig. 2-6 IP Configuration

• Managing 24 Port Gigabit Ethernet Switch through Ethernet Port

Before you communicate with the switch, you have to finish first the configuration of the IP address or to know the IP address of the switch. Then, follow the procedures listed below.

1. Set up a physical path between the configured switch and a PC by a qualified UTP Cat. 5 cable with RJ-45 connector.

   Note: If PC directly connects to the switch, you have to setup the same subnet mask between them. But, subnet mask may be different for the PC in the remote site. Please refer to Fig. 2-6 about the default IP address information.

2. Run web browser and follow the menu. Please refer to Chapter 3.

Fig. 2-7 the Login Screen for Web

2-1-4. IP Address Assignment

For IP address configuration, there are three parameters needed to be filled in. They are IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure is shown Fig. 2-8. It is "classful" because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of host refers to. And the host identifier must be unique in the same LAN. Here the term of IP address we used is version 4, known as IPv4.

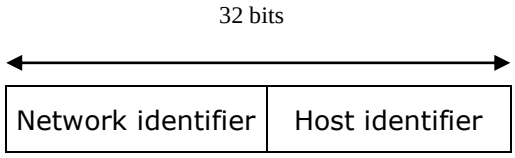
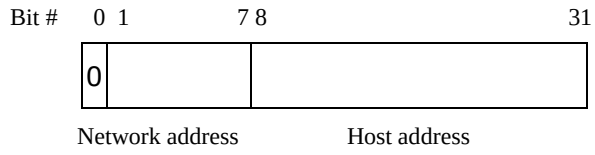


Fig. 2-8 IP address structure

With the classful addressing, it divides IP addresses into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/10. Each class has its address range described below.

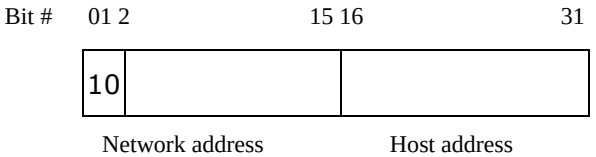
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



Class B:

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 (2^14)/16 networks able to be defined with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 (2^21)/24 networks able to be defined with a maximum of 254 (2^8 –2) hosts per network.

Class D and E:

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

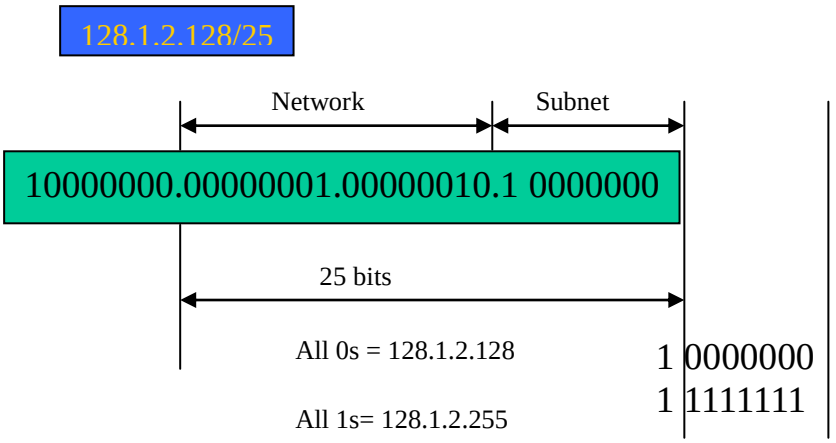
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and ease to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes is with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It’s too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that’s using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It’s now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's host number. For example, an IP address 128.1.2.128, what IP address reserved will be looked like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-3

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240.

This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For the routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as default router. Basically, it is a routing policy.

For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

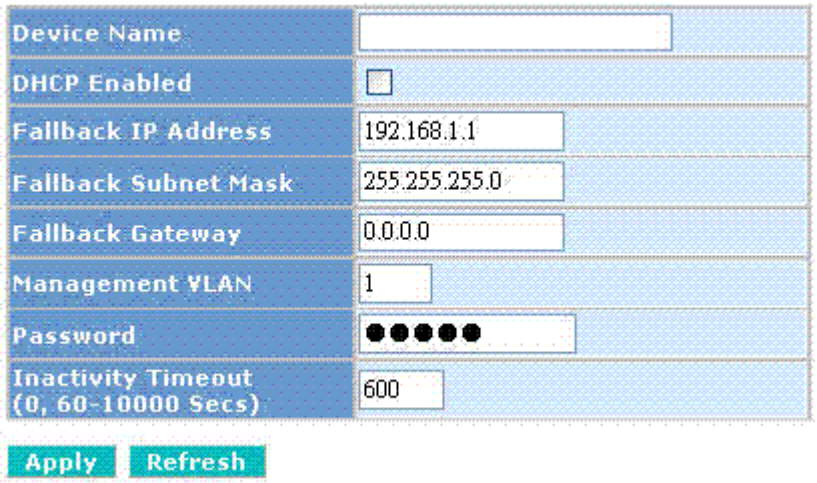


Fig. 2-8

First, IP Address: as shown in the Fig. 2-9, enter "192.168.1.1", for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown in the Fig. 2-9, enter "255.255.255.0". Any subnet mask such as 255.255.255.x is allowable in this case.

2-2. Typical Applications

The switch implements 24 Gigabit Ethernet TP ports with auto MDIX and four slots for the removable SFP modules. For more details on the specification of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

- Central site/remote site application is used in carrier or ISP (See Fig. 2-10)
- Peer-to-peer application is used in two remote offices (See Fig. 2-11)
- Office network(See Fig. 2-12)

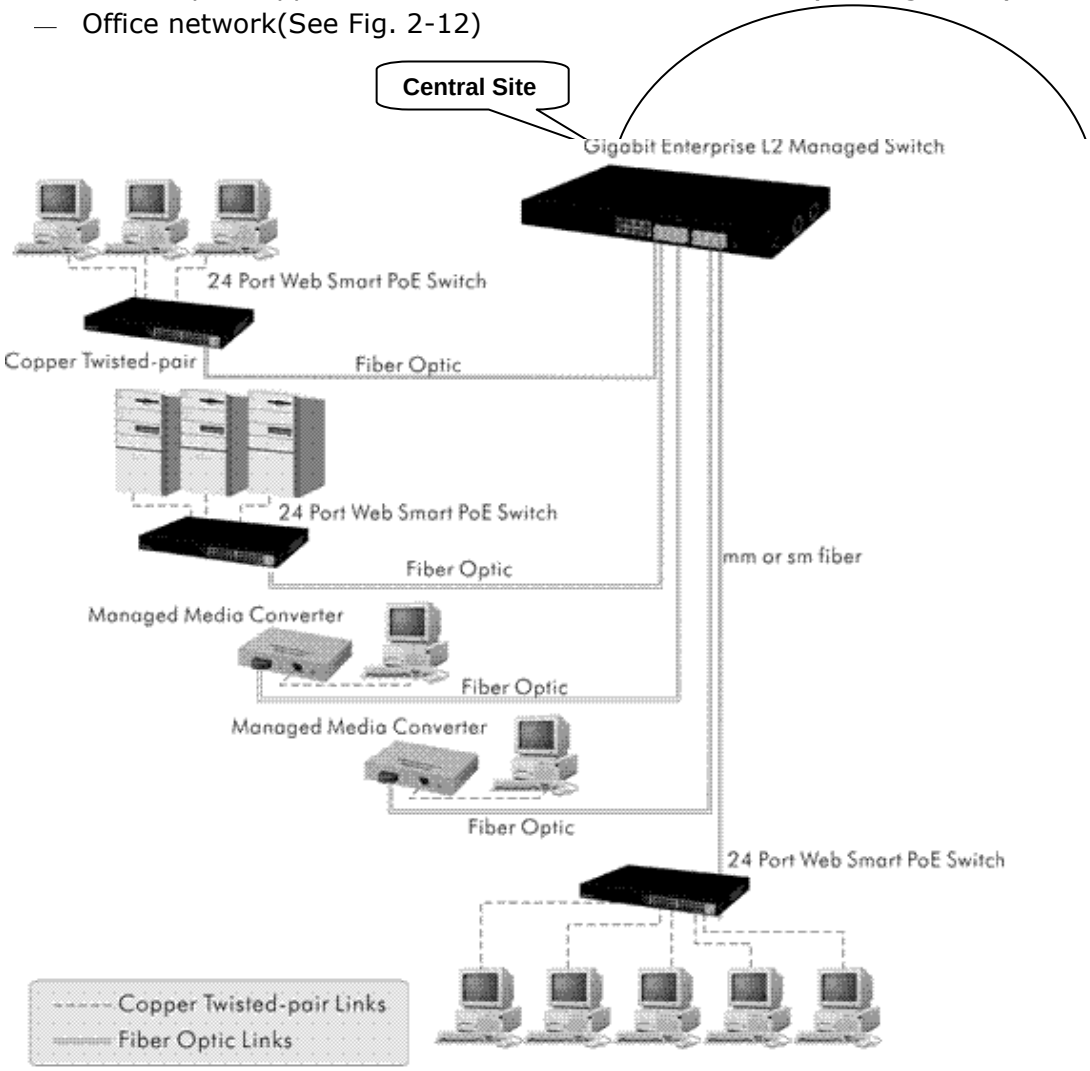


Fig. 2-10 Network Connection between Remote Site and Central Side

Fig. 2-10 is a system wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

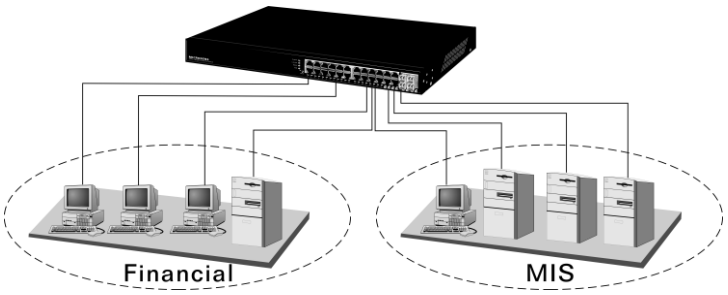


Fig. 2-11 Peer-to-peer Network Connection

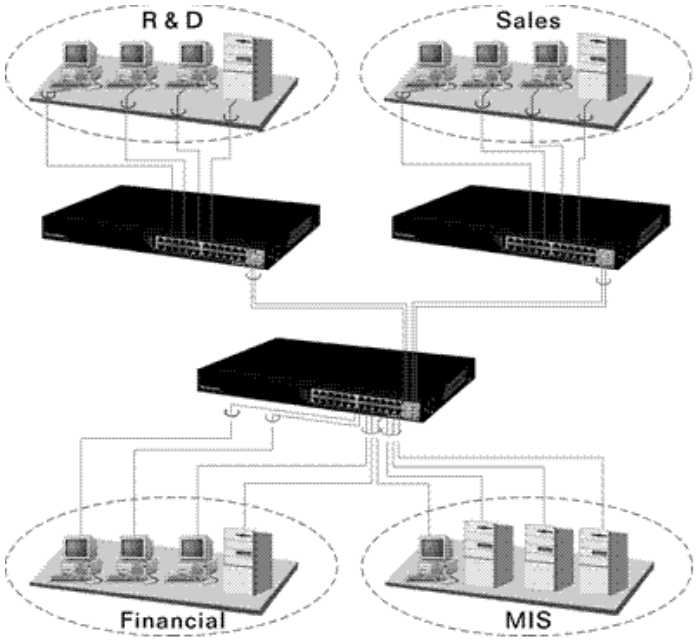


Fig. 2-12 Office Network Connection

3. Operation of Web-based Management

This chapter would introduce how to manage your Web Smart Switch and how to configure the 10/100/1000Mbps TP Ports and Gigabit SFP Fiber ports on the switch via web user interfaces. The Web Smart Switch provides 20 fixed Gigabit Ethernet TP ports and 4 Gigabit dual media ports. With this facility, you can easily access and monitor the status like port activity and multicast traffic through any ports on the switch.

The default values are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gate-way	192.168.1.253
Password	admin

Table 3-1

When the configuration of your switch is finished, you can browse it by the IP address you set up. For instance, type http://192.168.1.1 in the address row in a browser, then the following screen (see Fig.4-1) would show up and ask for your password input for login and access authentication. The default password is "admin". For the first time access, please enter the default password, and click **<Apply>** button. The login process now would be completed.

Web Smart Switch supports a simplified user management function which allows only one administrator to configure the switch at one time.

To optimize the display effect, we recommend Microsoft IE and 1024x768 display resolution.

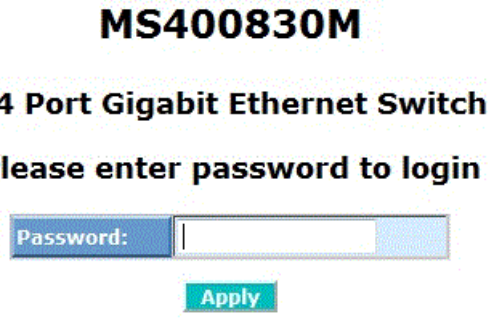


Fig. 3-1

3-1. Web Management Home Overview

After login, System Information would be displayed as Fig. 4-2 illustrated. This page lists default values and shows you the basic information of the switch, including "Switch Status", "TP Port Status", "Fiber Port Status", "Aggregation", "VLAN", "Mirror", "SNMP", and "Maximum Packet Length". With this information, you will know the software version, MAC address, ports available and so on. It would be helpful while malfunction occurred. For more details, please refer to Section 3-4-1.

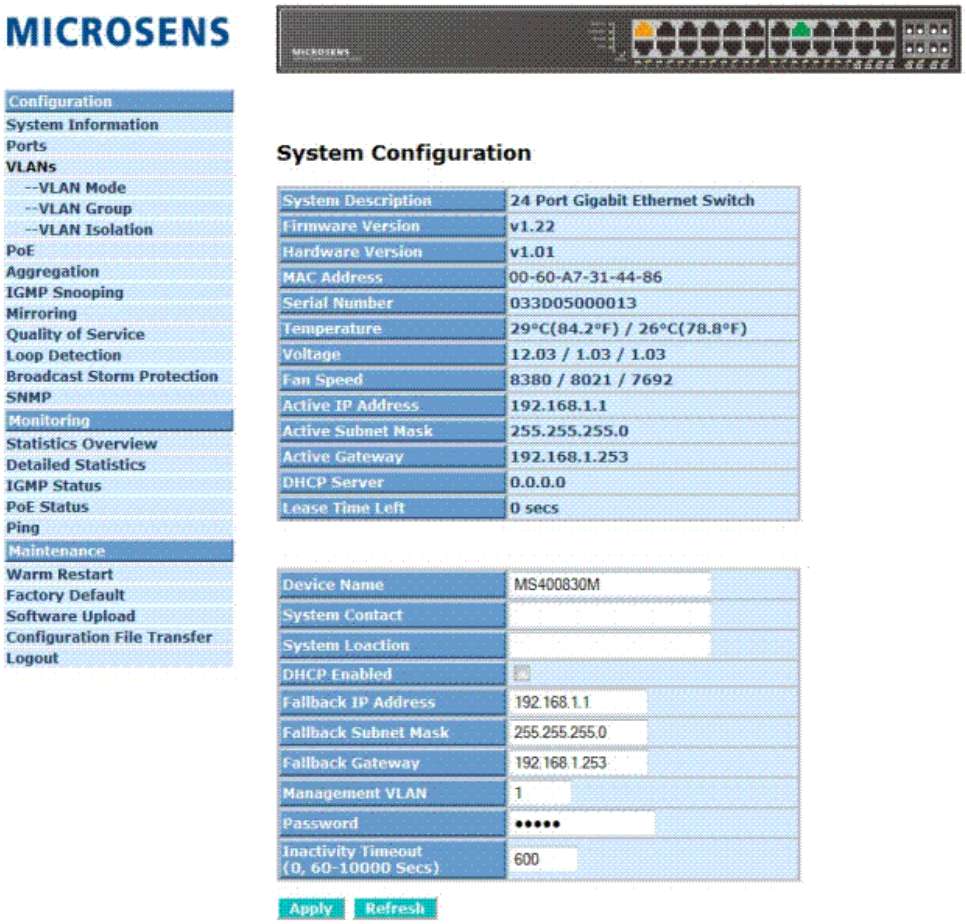
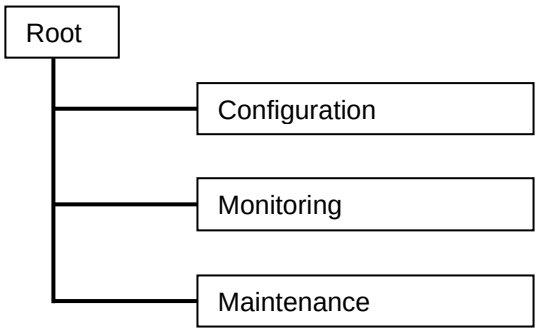


Fig. 3-2

3-1-1. Page Layout

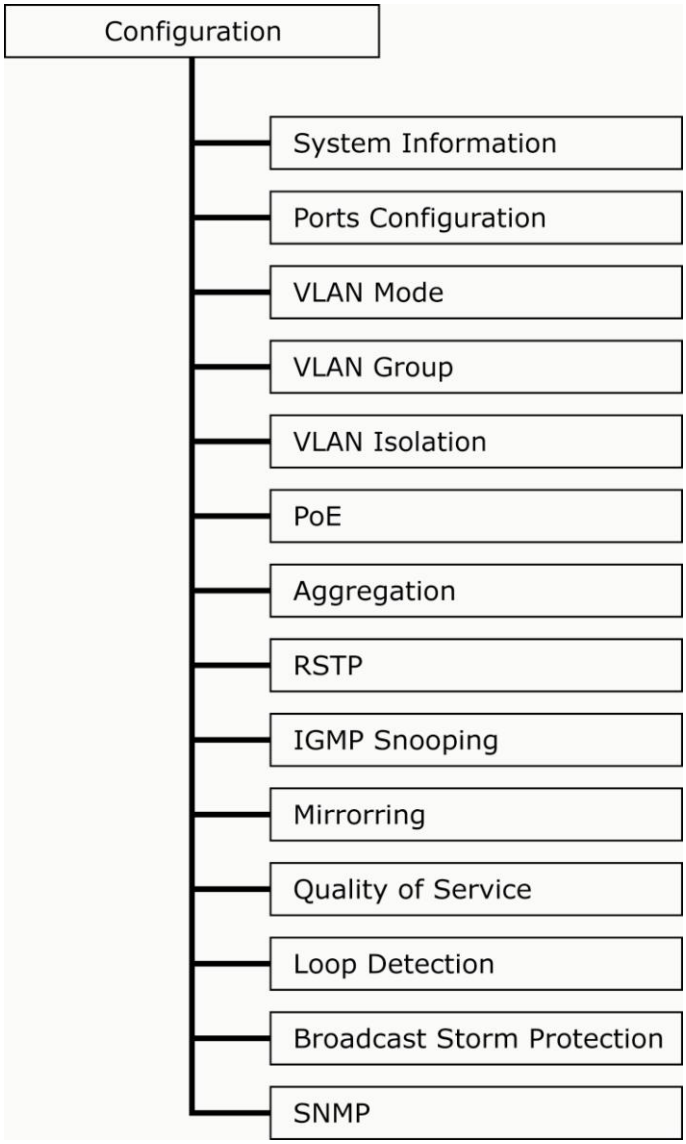
On the top part of the information page, it shows the front panel of the switch. Linked ports will be displayed in green color, and linked-off ones will be in black. For the optional modules, the slots with no module will only show covered plates, the other slots with installed modules would present modules. The images of modules would depend on the ones you insert. Vice versa, if ports are disconnected, they will show just in black.

On the left side, the main menu tree for web is listed in the page. According to the function name in boldface, all functions can be divided into three parts, including "Configuration", "Monitoring" and "Maintenance". The functions of each folder are described in its corresponded section respectively. As to the function names in normal type are the sub-functions. When clicking it, the function is performed. The following list is the main function tree for web user interface.



3-2. Configuration

Configuration includes the following functions: System Information, Ports Configuration, VLAN Mode Configuration, VLAN Group Configuration, VLAN Isolation, PoE, Aggregation, RSTP, IGMP Snooping, Mirroring, QoS, Loop Detection, Broadcast Strom Protection and SNMP.



3-2-1. System Information

System configuration is one of the most important functions. Without a proper setting, network administrator would not be able to manage the device. The switch supports manual IP address setting.

Fig. 3-3

Function name

System Configuration

Function description

Show system description, firmware version, hardware version, MAC address, serial number, active IP address, active subnet mask, active gateway, DHCP server and Lease time left.

Set device name, DHCP enable, fallback IP address, fallback subnet mask, fallback gateway, management VLAN, password and inactivity timeout.

Parameter description

System Description:

The simple description of this switch

Firmware Version:

The firmware version of this switch

Hardware Version:

The hardware version of this switch

MAC Address:

It is the Ethernet MAC address of the management agent in this switch.

Serial Number:

The serial number is assigned by the manufacturer.

Active IP Address:

Show the active IP address of this switch.

Active Subnet Mask:

Show the active subnet mask of this switch.

Active Gateway:

Show the active gateway of this switch.

DHCP Server:

Show the IP address of the DHCP server.

Default: 0.0.0.0

Lease Time Left:

Show the lease time left of DHCP client.

Device Name:

Set a special name for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character and null are acceptable.

Default: Giga Switch

System Contact:

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Location:

This entry informs about the physical location of this node. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

DHCP Enabled:

Enable DHCP snooping, just tick the check box (☑) to enable it. If this function is enabled the IP settings are automatically assigned by a DHCP server. Please ensure that a DHCP server is available via the network.

Default: disabled

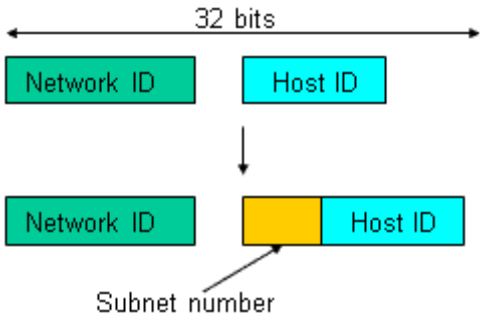
Fallback IP Address:

Users can configure the IP settings and fill in new values. Then, click **<Apply>** button to update.

Default: 192.168.1.1

Fallback Subnet Mask:

Subnet mask is made for the purpose to get more network addresses because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can't communicate with other devices each other. But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount of 2 power of the bit number of subnet number (2^(bit number of subnet number)).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

For more information, please also see the Section 2-1-4 "IP Address Assignment" in this manual.

Default: 255.255.255.0

Fallback Gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

Management VLAN:

Show the management VLAN number.

Password:

Set a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable.

Default: admin

Inactivity Timeout (sec):

Set the auto-logout timer. The valid value is 0 ~ 60 in the unit of minute and a decimal point is not allowed. The value 0 means auto-logout timer is disabled.

Default: 0

3-2-2. Port Configuration

Function name

Port Configuration

Function description

Port Configuration is applied for the settings of the ports on the switch. By this function, you can set or reset the values for mode and Flow Control.

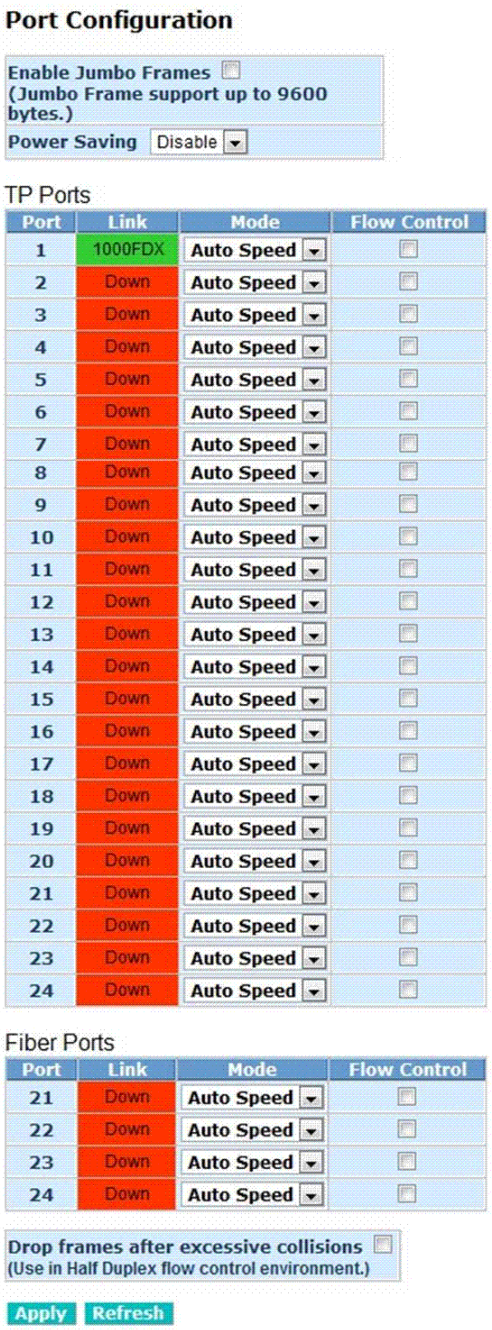


Fig. 3-4 Port Configuration

Parameter description

Enable Jumbo Frames:

This function support jumbo frames of up to 9600 bytes. Just tick the check box (☑) to enable it.

Default: disabled

Perfect Reach/Power Saving Mode:

This function supports Power Saving and perfect Reach, Just select with the Full/ Link-up/ Link-down/ Disable

Default: disable

Link:

Show link status of this port.

Mode:

Set the speed and duplex of the port. If the media is 1 Gbps fiber, there are three modes to choose: Auto Speed, 1000 Full and disable. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

Default: auto speed mode

Flow Control:

Flow control is a mechanism to tell the source device stopping sending frame for a specified period of time designated by target device until the PAUSE time expires. This is accomplished by sending a PAUSE frame from target device to source device. When the target is not busy and the PAUSE time is expired, it will send another PAUSE frame with zero time-to-wait to source device. After the source device receives the PAUSE frame, it will again transmit frames immediately. PAUSE frame is identical in the form of the MAC frame with a pause-time value and with a special destination MAC address 01-80-C2-00-00-01. As per the specification, PAUSE operation cannot be used to inhibit the transmission of MAC control frame.

You can just tick the check box (☑) to enable flow control. If flow control is enabled, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is disabled, there will be no flow control in the port. It drops the packet if too much to handle.

Default: disabled

3-2-3. VLAN Mode Configuration

Web Smart Switch supports Port-based VLAN and Tag-based VLAN (802.1q). Its VLAN mode supports 16 active VLANs and the available VLAN ID range is from 1~4094. VLAN configuration is used to divide a LAN into smaller ones. With proper configuration, you can gain not only improved security and increased performance, but also save a lot of VLAN management effort.

Function name

VLAN Mode Setting

Function description

The VLAN Mode Selection function includes four modes: Port-based, Tag- based, Metro mode or Disable, you can choose one of them by pulling down list and pressing the **<Downward>** arrow key. Then, click **<Apply>** button, the settings will take effect immediately.

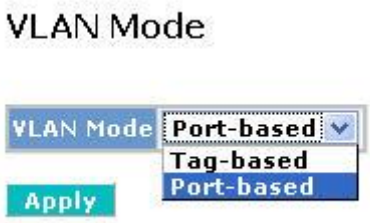


Fig. 3-5 Select VLAN Mode

Parameter description

VLAN Mode:

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 16 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q.

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 4094 Tag VLAN groups.

3-2-4. VLAN Group Configuration

Function name

Tag-based VLAN Configuration (Tag based VLAN mode)

Function description

The VLAN membership configuration for the selected switch can be monitored and modified here. Up to 16 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

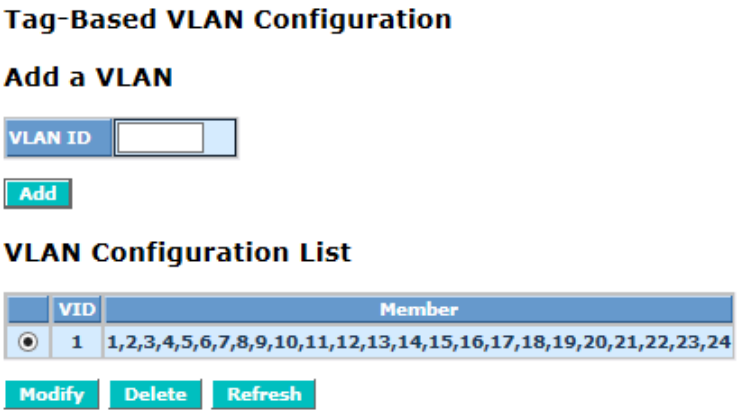


Fig. 3-5-1 tag- VLAN Mode

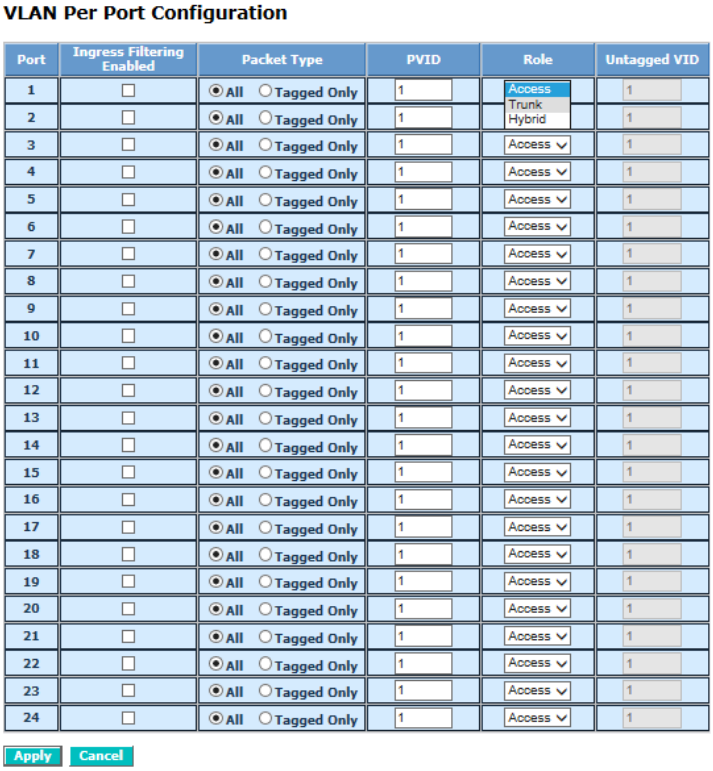


Fig. 3-5-2 Per port configuration

Parameter description

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based mode.

Member:

In modify function this is used to enable or disable if a port is a member of the new added VLAN, "Enabled" means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

Port:

Port number

Ingress Filtering Enabled:

Discard other VLAN group packets, only forward this port joined VLAN group packets.

VLAN aware Enabled:

Discard other VLAN group packets, only forward this port joined VLAN group packets.

Packet Type:

All:

Forward all tagged and untagged packets.

Tagged Only:

Forward tagged packets only and discard untagged packets.

PVID:

This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID

Role:

This is an egress rule of the port. Here you can choose Access, Trunk or Hybrid. Trunk means the outgoing packets must carry VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. As to Hybrid, it is similar to Trunk, and both of them will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untagged VID of this port.

Untagged VID:

Valid range is 1~4094. It works only when role is set to Hybrid.

Function name

Port-based VLAN configuration (Port-based VLAN mode)

Function description

It shows the information of VLAN groups, and allows administrators to maintain them by modifying and deleting each VLAN group. User also can add a new VLAN group by inputting a new VLAN name and VLAN ID.

If you are in port-based VLAN, it will just show the ID、Member of the existed port-based VLAN group. If you are in tag-based VLAN, it will show the ID, VID and member of the existed tag-based VLAN group. The switch can store the configuration of port-based VLAN and tag-based VLAN separately. When you choose one of VLAN mode, the switch will bring you the responded VLAN configuration which keeps the default data. You can easily create and delete a VLAN group by pressing **<Add>** and **<Delete>** function buttons, or clicking the Group ID directly to edit it.

Fig. 3-6 Port-Based VLAN Configuration

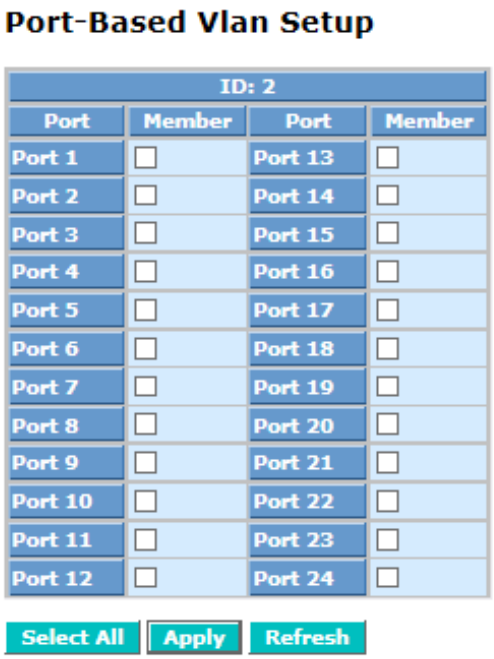


Fig. 3-7 Add or Remove VLAN Member

Parameter description

ID (Group ID):

When you want to edit a VLAN group, you must select the Group ID field. Then, you will enter Tag Base VLAN Group Setting or Port Base VLAN Group Setting page, which depends on your VLAN mode selection.

Member:

In modify function this is used to enable or disable if a port is a member of the new added VLAN, "enabled" means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

Add Group:

Create a new port-based VLAN or tag-based VLAN, which depends on the VLAN mode you choose in VLAN mode function.

Delete Group:

Just tick the check box (☑) beside the ID, then press the **<Delete>** button to delete the group.

3-2-5. VLAN Port Isolation Configuration

Function name

Port Isolation Configuration

Function description

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address of a data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address of the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

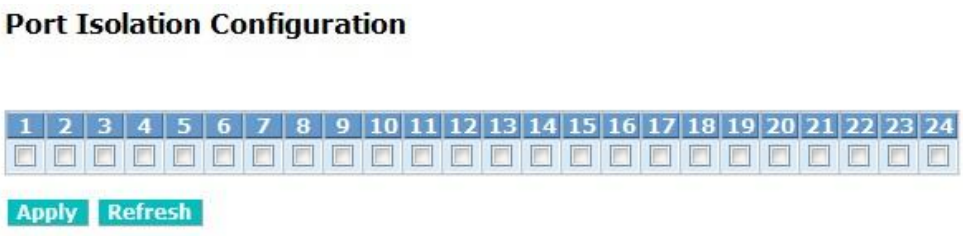


Fig. 3-9 Port Isolation configuration

Parameter description

Port Members:

A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

3-2-6. PoE

Power over Ethernet (PoE) technology allows IP telephones, wireless LAN access points, and other powered devices (PDs) to receive power and transfer data over existing LAN cabling.

Function name

Power over Ethernet configuration

Function description

In PoE Port Management function, user can configure the settings about PoE.

The switch complies with IEEE 802.3af protocol and is capable of detecting automatically that whether the device linked to the port on the switch is PD (Powered Device) or not. The switch also manages the power supplement based on the class of the PD, and it will stop supplying the power once the power required by the PD excesses the class, short circuit or over temperature occurs.

PoE (Power over Ethernet) Configuration

Port	PoE Enabled	Priority	Allocation [W]	Detection	Delay Time (0~300; 0:Disable)	Reset
1	☑	Low	15.4	4-Point	0 Second(s)	☐
2	☑	Low	15.4	4-Point	0 Second(s)	☐
3	☑	Low	15.4	4-Point	0 Second(s)	☐
4	☑	Low	15.4	4-Point	0 Second(s)	☐
5	☑	Low	15.4	4-Point	0 Second(s)	☐
6	☑	Low	15.4	4-Point	0 Second(s)	☐
7	☑	Low	15.4	4-Point	0 Second(s)	☐
8	☑	Low	15.4	4-Point	0 Second(s)	☐
9	☑	Low	15.4	4-Point	0 Second(s)	☐
10	☑	Low	15.4	4-Point	0 Second(s)	☐
11	☑	Low	15.4	4-Point	0 Second(s)	☐
12	☑	Low	15.4	4-Point	0 Second(s)	☐
13	☑	Low	15.4	4-Point	0 Second(s)	☐
14	☑	Low	15.4	4-Point	0 Second(s)	☐
15	☑	Low	15.4	4-Point	0 Second(s)	☐
16	☑	Low	15.4	4-Point	0 Second(s)	☐
17	☑	Low	15.4	4-Point	0 Second(s)	☐
18	☑	Low	15.4	4-Point	0 Second(s)	☐
19	☑	Low	15.4	4-Point	0 Second(s)	☐
20	☑	Low	15.4	4-Point	0 Second(s)	☐
21	☑	Low	15.4	4-Point	0 Second(s)	☐
22	☑	Low	15.4	4-Point	0 Second(s)	☐
23	☑	Low	15.4	4-Point	0 Second(s)	☐
24	☑	Low	15.4	4-Point	0 Second(s)	☐

Apply Refresh

Fig. 3-10

Parameter description

PoE Enabled:

PoE can be enabled or disabled for each port separately.

Priority:

Three options are offered for the user to choose, including Normal, Low and High. Default is Normal. The switch will stop supplying the power to the port based on the order of the priority Low→Normal→High in case total power required by all PDs linked to the switch excesses the power limit. As the ports have the same priority, then the switch will cease the power supplement from the port with the highest port id (12→1).

Allocation (W):

The power is consumed by the port.

Detection:

The detection represents the PoE capacitor detection for the port.

Legacy: Legacy capacitive detection only

4-point: IEEE 802.3af 4-point detection only

Both: IEEE 802.3af 4-point detection followed by Legacy detection

Delay time:

The delay time is using for set the time period for PD PoE enable time delay period. It is a solution to avoid rush current to cause shorter PD. The available time period is from 0 to 300 seconds and 0 means disable the function

Reset Port:

To reset the port PoE configuration and status

3-2-7. Aggregation

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle ports by same speed, MAC, and full duplex to be a single logical port, thus the logical port can aggregate the bandwidth of these ports. This means you can apply your current Ethernet equipment to build the bandwidth aggregation. For example, if three Fast Ethernet ports are aggregated into a logical port, then this logical port's bandwidth would be as three times high as a single Fast Ethernet port.

Function name

Aggregation Configuration

Function description

Display the current setup of Aggregation Trunking. With this function, user is allowed to add a new trunking group or modify the members of an existed trunking group.

The load balance mechanism is based on MAC SA/DA hash algorism and it is not configurable.

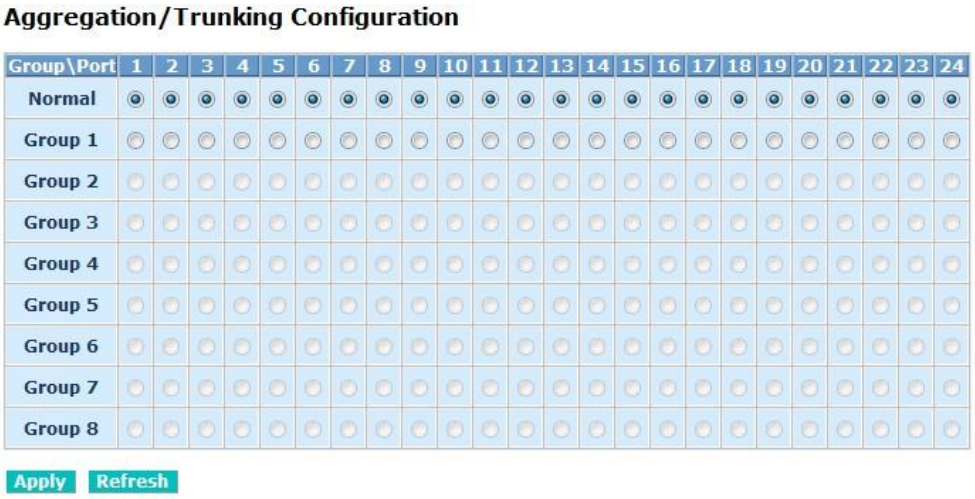


Fig. 3-11 Aggregation / Trunking Configuration

Parameter description

Normal:

Set up the ports that do not join any aggregation trunking group.

Group 1~8:

Group the ports you choose together. Up to 2 to 12 ports can be selected for each group.

3-2-8. RSTP

RSTP detects and resolves network loops, and provides backup links between switches, bridges and routers. The protocol allows a switch to communicate with other RSTP compliant switches, and to ensure only one path existing between two stations in your network environment.

The switch allows you to create multiple STP configurations and assign ports to a specific tree.

RSTP can be used together with VLANs. Regardless of the VLAN settings all BPDUs are sent untagged.

Please take care that other switches are configured accordingly. Especially other MICROSENS switches with RSTP VLAN have to be configured in a way that the RSTP VLAN is sent untagged.

Function name

RSTP System Configuration

Function description

This screen is used to display the RSTP system configuration and set the need of parameters.

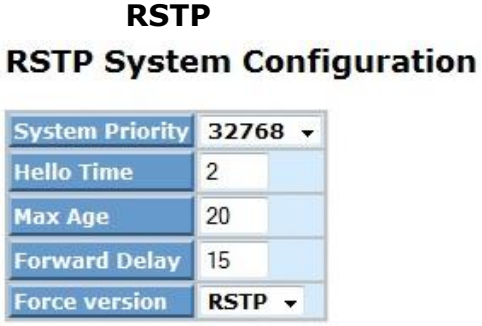


Fig. 3-12 RSTP System Configuration

Parameter description

System Priority:

System priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a vale from the drop-down list box.
The lower the numeric value you assign, the higher the priority for this system.

Default: 32768

Hello Time:

This is the time interval in seconds between BPDU configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Default: 2

Max Age:

This is the maximum time a switch can wait without receiving a BPDU before attempting to reconfigure. The allowed range is 6 to 40 seconds.

Default: 20

Forward Delay:

This is the maximum time (in seconds) a switch will wait before changing states. The general rule: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)

Default: 15

Force version:

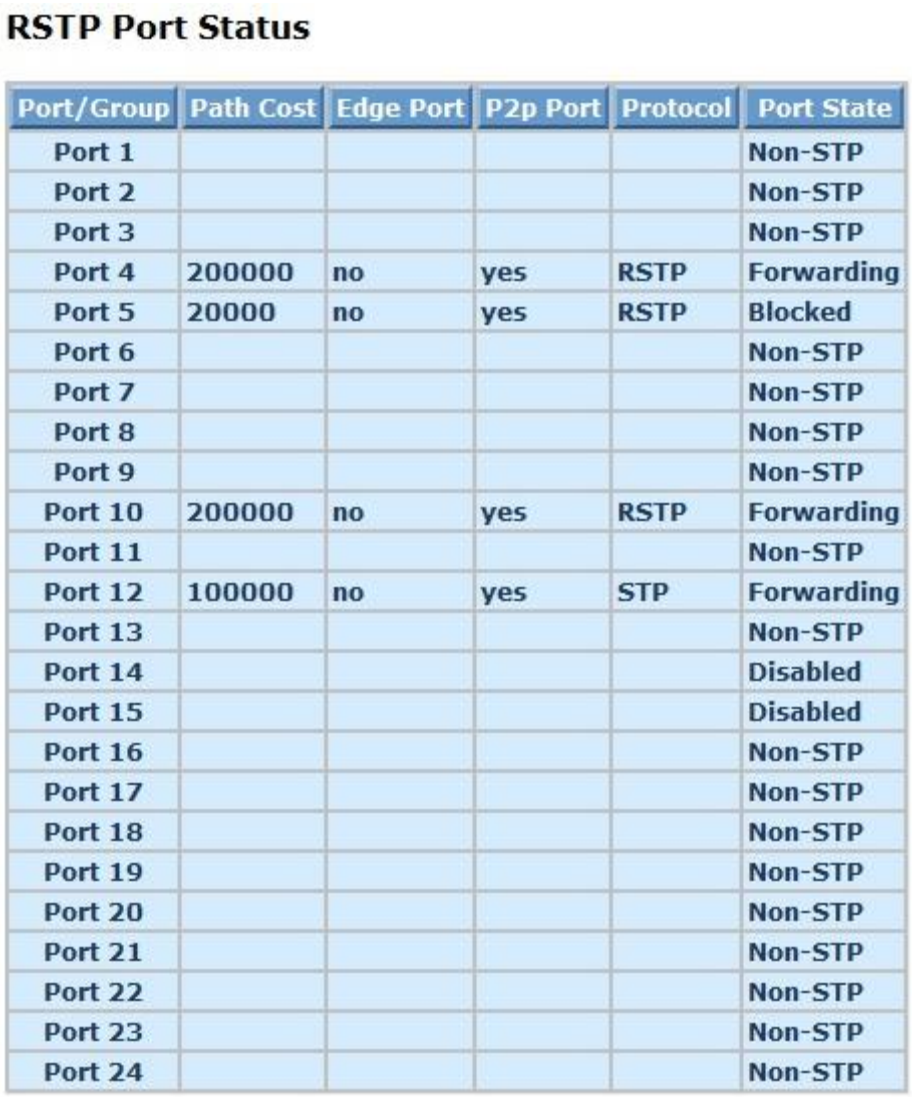
Select RSTP or STP protocol from the drop-down list box.

Function name

RSTP Port Configuration

Function description

Enable or disable RSTP protocol on the ports that are selected and set path cost.



RSTP Port Status

Port/Group	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1					Non-STP
Port 2					Non-STP
Port 3					Non-STP
Port 4	200000	no	yes	RSTP	Forwarding
Port 5	20000	no	yes	RSTP	Blocked
Port 6					Non-STP
Port 7					Non-STP
Port 8					Non-STP
Port 9					Non-STP
Port 10	200000	no	yes	RSTP	Forwarding
Port 11					Non-STP
Port 12	100000	no	yes	STP	Forwarding
Port 13					Non-STP
Port 14					Disabled
Port 15					Disabled
Port 16					Non-STP
Port 17					Non-STP
Port 18					Non-STP
Port 19					Non-STP
Port 20					Non-STP
Port 21					Non-STP
Port 22					Non-STP
Port 23					Non-STP
Port 24					Non-STP

Fig. 3-13 RSTP Port Configuration

Parameter description

Protocol Enabled:

Just tick the check box (☑) beside the port x to enable RSTP protocol, then press the **<Apply>** button to apply.

Edge:

Just tick the check box (☑) beside the port x to enable edge function.

Path Cost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost, user can select auto or set the rage from 1 to 200000000.

3-2-9. IGMP Snooping

Function name

IGMP Snooping Configuration

Function description

IGMP Snooping lets administrators configure a switch to constrain multicast traffic by listening to Internet Group Management Protocol (IGMP). After finishing the settings, please press **<Apply>** button to start up the function.

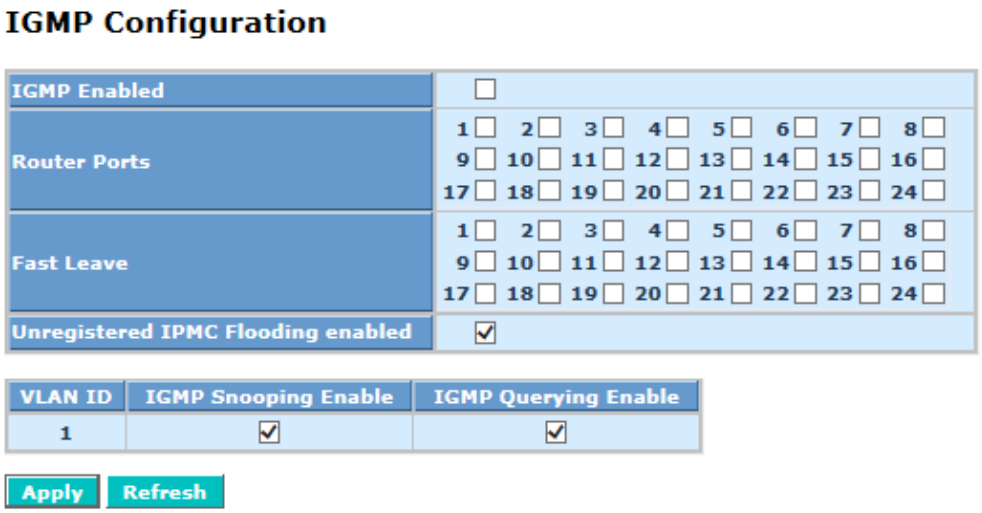


Fig. 3-14 IGMP Configuration

Parameter description

IGMP Enabled:

Just tick the check box (☑) to enable this function.

Default: disabled

Router Ports:

The router ports setting means all IGMP report packets from clients, they will be forwarded to specific port to IGMP server connected router. Prevent IGMP report transform broadcast to avoid unnecessary bandwidth waste.

Just tick the check box (☑) beside the port x to enable router ports, then press the **<Apply>** button to start up.

Default: none

Fast Leave:

Enable the fast leave on the port.

Unregistered IGMP Flooding enabled:

Just tick the check box (☑) to enable this function.

Default: enabled

VLAN ID:

At the IGMP Enable mode being selected, it will list the VLAN ID number.

IGMP Snooping Enabled:

After IGMP Enabled function start up then user can tick the check box (☑) to enable this function.

Default: enabled

IGMP Querying Enabled:

After IGMP Enabled function start up then user can tick the check box (☑) to enable this function.

Default: enabled

3-2-10. Mirroring Configuration

Function name

Mirror Configuration

Function description

Mirror Configuration is provided to monitor the traffic in the network. This switch supports one-port mirror multi-ports. For example, we assume that port A and port B are source ports, and port C is mirror port respectively, thus, the traffic passing through port A and port B will be copied to port C for monitor purpose.

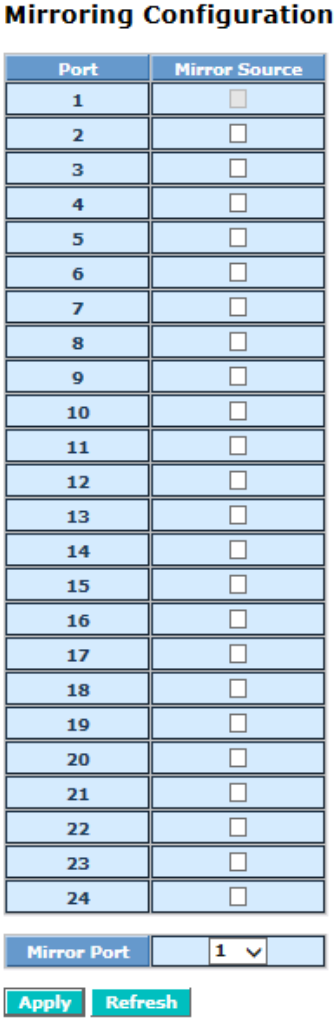


Fig. 3-15 Mirror ports configuration

Parameter description

Source Port:

Set up the port for being monitored. Just tick the check box (☑) beside the port x and valid port is Port 1~24.

Mirror Port: Use the drop-down menu to select a mirror port.

3-2-11. QoS (Quality of Service) Configuration

The switch offers powerful QoS function. This function supports VLAN-tagged priority that can make precedence of 8 priorities, and DSCP (Differentiated Services Code Point) on Layer 3 of network framework.

Fig. 3-16 QoS Configuration

Function name

QoS Configuration

Function description

While setting QoS function, please select QoS mode in drop-down menu at first. Then you can use 802.1p priority and DSCP priority functions. In this function, you can enable/disable QoS mode and set priority control, such as: 802.1p and DSCP. The switch only supports strict priority. High priority queue is always passed first.

Function name

802.1p QoS mode

Function description

This function will affect the priority of VLAN tag. Based on priority of VLAN tag, it can arrange 0~7 priorities, priorities can map to 4 queues of the switch (low, normal, medium, high) and possess different bandwidth distribution according to your weight setting.

Parameter description

Prioritize Traffic:

Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.

Port Number:

When Custom is selected for Prioritize Traffic, you may assign specific port number for 802.1p Configuration.

802.1p Configuration:

Each priority can select any of queues. In default, priority 0 is mapping to queue normal, priority 1 is mapping to queue low, priority 2 is mapping to queue low, priority 3 is mapping to queue normal, priority 4 is mapping to queue medium, priority 5 is mapping to queue medium, priority 6 is mapping to queue high, and priority 0 is mapping to queue high.

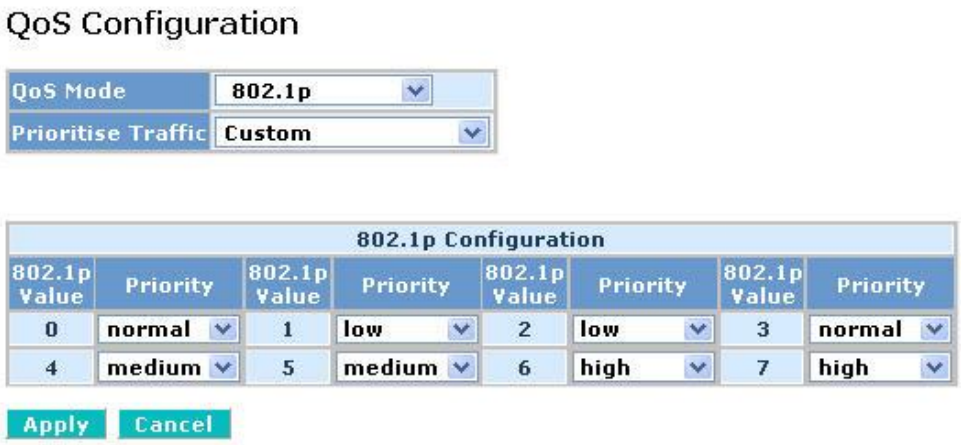


Fig. 3-17 802.1p Setting

Function name

DSCP QoS mode

Function description

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of traffic class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of class that belong to any of queue (low, normal, medium, high).

Parameter description

Prioritize Traffic:

Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.

Port Number:

When Custom is selected for Prioritize Traffic, you may assign specific port number for DSCP configuration.

DSCP Configuration:

64 kinds of priority traffic as mentioned above, user can set up any of queue (low, normal, medium, high). In default, priority 0~63 are mapping to queue high.

Fig. 3-18 DSCP Setting

3-2-12. Loop Detection

Function name

Loop Detection Configuration

Function description

The loop detection is used to detect the presence of traffic. When switch receives packet's (looping detection frame) MAC address the same as oneself from port, show Loop detection happens. The port will be locked when it received the looping detection frames. If you want to resume the locked port, please find out the looping path and take off the looping path, then select "Unlock port" and click on "Apply" to turn on the locked ports.

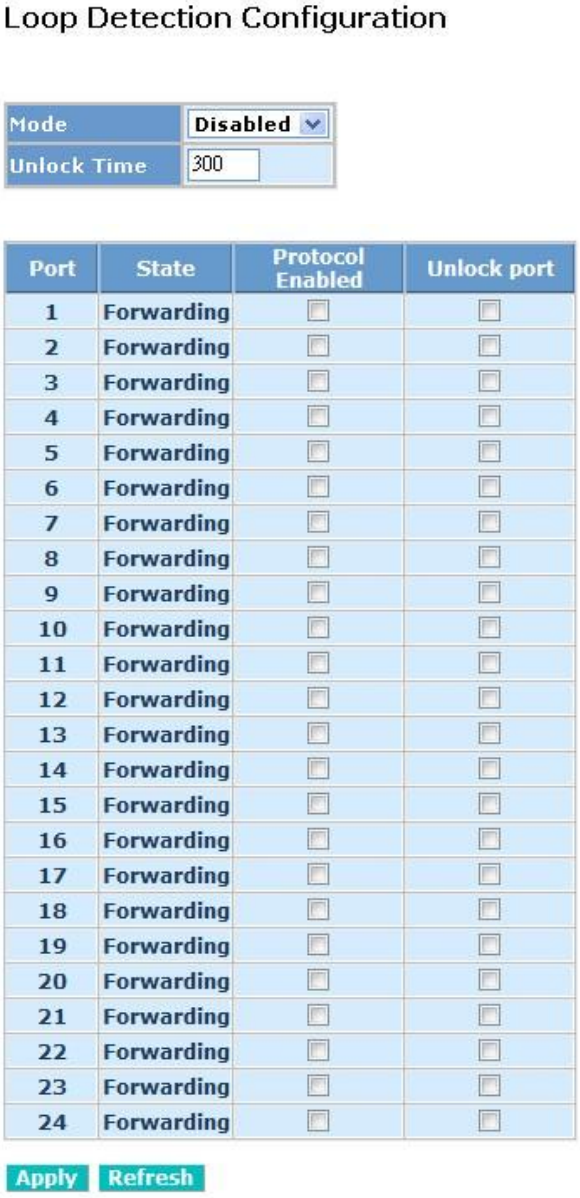


Fig. 3-19 Loop Detection Configuration

Parameter description

Mode:

Controls whether Loop Detection is enabled (as a whole).

Unlock Time:

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action is to shut down the port).

State:

Show the status of this port.

Protocol Enabled:

Controls whether Loop Detection is enabled on this switch port

When port number is chosen and enable port's Loop Detection, the port can detect loop happens and port will be locked. If loop did not happen, port maintains unlocked.

Unlock port:

When ticking the port, port locked will be opened and turned into unlocked. If not ticking the port, port maintains locked.

3-2-13. Broadcast Strom Protection

Function name

Broadcast Strom Protection configuration

Function description

When the broadcast packets received by the switch exceed the threshold configured, the port will be blocked for a period of time which can be set. After a configured time, the switch will detect whether the broadcast packets received on the port still exceed the threshold. If the broadcast traffic is still higher than, the port will be closed for a period of time again. If the broadcast traffic is under the threshold, the port will re-open and forward the packets normally.

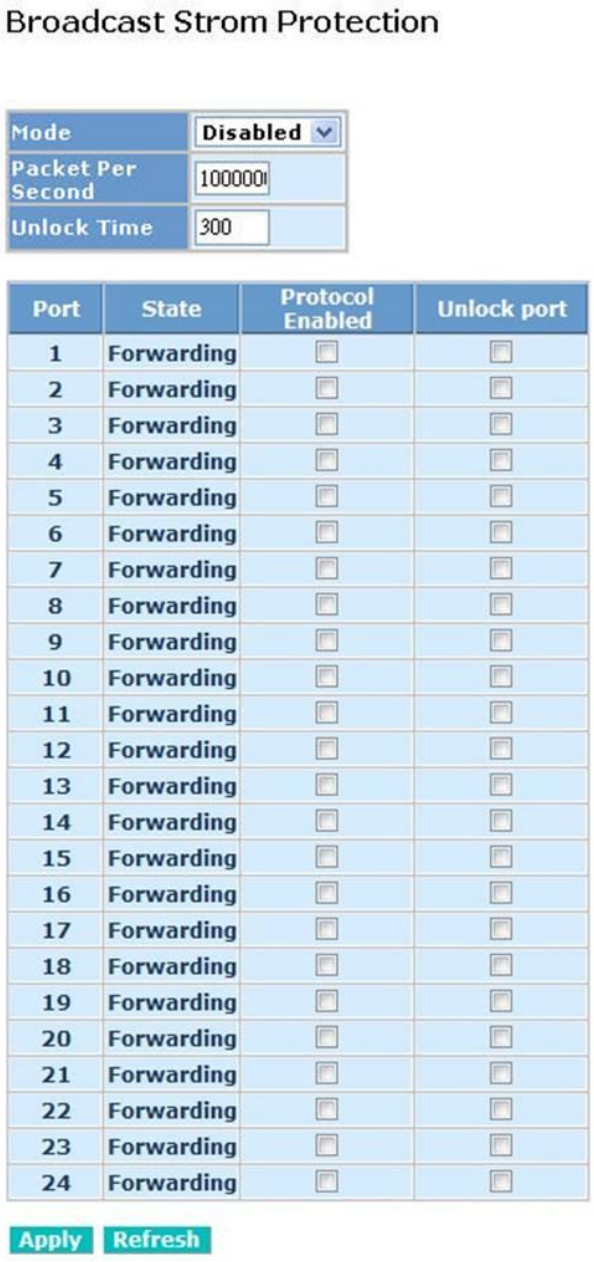


Fig. 3-20 Rate Limit Configuration

Parameter description

Mode:

Controls whether Broadcast Strom Protection is enabled (as a whole)

Packet Per Second:

It is a threshold. When the broadcast packet traffic in a second is higher than the threshold configured, Broadcast Strom Protection will disable the port.

Unlock Time:

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action is to shut down the port).

State:

Show the status on the port.

Protocol Enabled:

Controls whether Broadcast Strom Protection is enabled on this switch port

Unlock port:

When ticking the port, port locked will be opened and turned into unlocked. If not ticking the port, Port maintains locked.

3-2-14. SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. It is a protocol used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Function name

SNMP Configuration

Function description

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, and then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click **<Apply>** button, the setting takes effect.

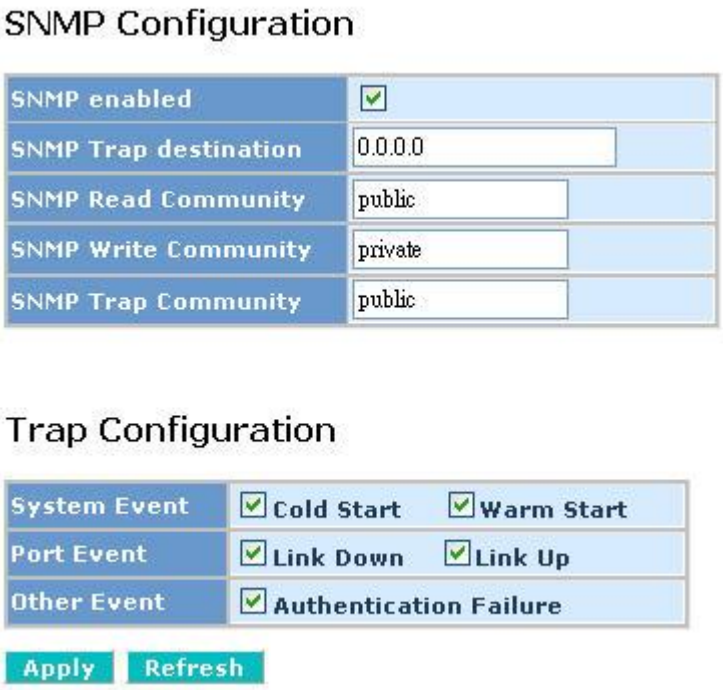


Fig. 3-21 SNMP Configuration

Parameters description:

SNMP enable:

The term SNMP enable here is used for the activation or de-activation of SNMP. Default is "Disabled".

Read/Write/Trap Community:

Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don't

have the same community name, they don't belong to the same group. Hence, the requesting network management unit cannot access the device with different community name via SNMP protocol; if they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is not allowed to put any blank in the community name string. Any printable character is allowable.

The community name for each function works independently. Each function has its own community name. Say, the community name for Read only works for Read function and can't be applied to other function such as Write and Trap.

Default SNMP function: Disabled

Default community name for Read: public

Default community name for Write: private

Default community name for Trap: public

System Event:

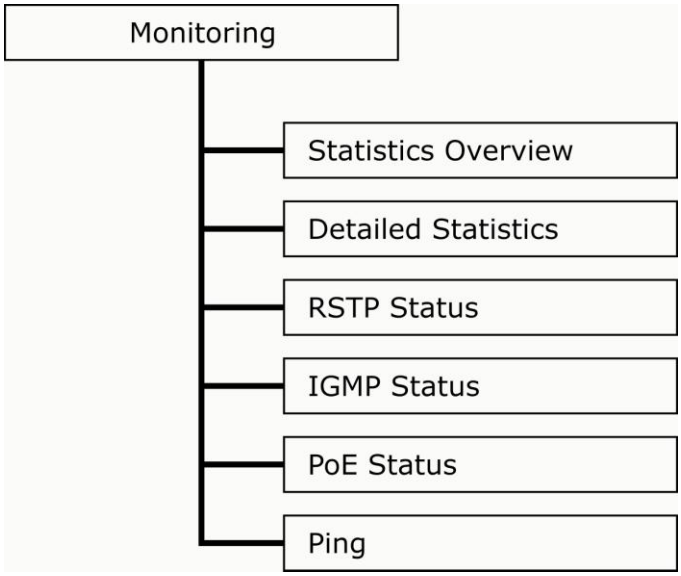
The System Event trap enable here is used for the "Cold Boot" or "Warm Boot" of System Event. Default is "Disabled".

Port Event:

The "Port Event Trap Enable" button here is used for the "Link Up" or "Link Down" of system Event. Default is "Disabled".

3-3. Monitoring

There are six functions contained in the monitoring function.



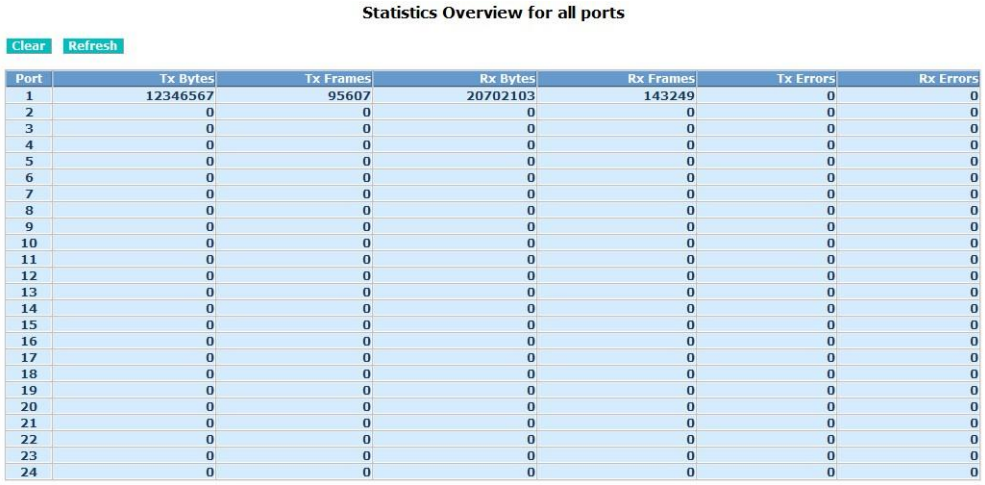
3-3-1. Statistics Overview

Function name

Statistics Overview for all ports

Function description

The section describes to the port statistics information and provides overview of general traffic statistics for all switch ports.



Statistics Overview for all ports

Clear Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	12346567	95607	20702103	143249	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	0	0	0	0	0	0

Fig. 3-22 Statistics Overview for all ports

Parameter description

Tx/Rx Bytes:

The number of received and transmitted bytes per port

Tx/Rx Frames:

The number of received and transmitted frames per port.

Tx/Rx Errors:

The number of frames received in error and the number of incomplete transmissions per port.

3-3-2. Detailed Statistics

Function name:

Detailed Statistics

Function description:

Display the detailed counting number of each port's traffic. In the Fig. 4-21, the window can show all counter information each port at one time.

Receive Total		Transmit Total	
Rx Packets	143722	Tx Packets	95923
Rx Octets	20767316	Tx Octets	12387330
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	14443	Tx Broadcast	3
Rx Multicast	2099	Tx Multicast	0
Rx Broad- and Multicast	-	Tx Broad- and Multicast	-
Rx Error Packets	0	Tx Error Packets	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	105355	Tx 64 Bytes	71762
Rx 65-127 Bytes	24694	Tx 65-127 Bytes	11859
Rx 128-255 Bytes	5170	Tx 128-255 Bytes	1
Rx 256-511 Bytes	12219	Tx 256-511 Bytes	16
Rx 512-1023 Bytes	12826	Tx 512-1023 Bytes	11967
Rx 1024- Bytes	0	Tx 1024- Bytes	321
Receive Error Counters		**Transmit Error Counters**	
Rx CRC/Aligment	0	Tx Collisions	0
Rx Undersize	0	Tx Drops	0
Rx Oversize	0	Tx Overflow	-
Rx Fragments	0		
Rx Jabber	0		
Rx Drops	0		

Fig. 3-23 Detailed Statistics for each port

Parameter description:

Rx Packets:

The counting number of the packet received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

Show the counting number of the received broadcast packet.

Rx Multicast:

Show the counting number of the received multicast packet.

Rx Broad- and Multicast:

Show the counting number of the received broadcast with multicast packet.

Rx Error Packets:

Show the counting number of the received error packets.

Tx Packets:

The counting number of the packet transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

Show the counting number of the transmitted broadcast packet.

Tx Multicast:

Show the counting number of the transmitted multicast packet.

Tx Broad- and Multicast:

Show the counting number of the transmitted broadcast with multicast packet.

Tx Error Packets:

Show the counting number of the received error packets.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC

Rx Oversize:

Number of long frames (according to max_length register) with valid CRC

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC

Rx Jabber:

Number of long frames (according to max_length register) with invalid CRC

Rx Drops:

Frames dropped due to the lack of receiving buffer.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx Overflow:

Number of frames dropped due to the lack of transmitting buffer.

3-3-4. RSTP Status

Function name

RSTP VLAN Bridge Overview

Function description

This screen informs about general RSTP settings and shows the current status of the Spanning Tree including root bridge and root port.

Fig. 3-24 RSTP VLAN Bridge Overview

Parameter description

Bridge ID:

Displays ID of this device

Bridge Priority:

Displays priority settings of this device

Root ID:

Displays ID of the root bridge

Root Priority:

Displays priority of the root bridge

Root Port:

The port which is part of the active path to the root bridge

Hello Time:

This is the time interval in seconds between BPDU configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Max Age:

This is the maximum time a switch can wait without receiving a BPDU before attempting to reconfigure. The allowed range is 6 to 40 seconds.

Forward Delay:

This is the maximum time (in seconds) a switch will wait before changing states.

Topology:

Informs about current status of the spanning tree topology

Function name

RSTP Port Configuration

Function description

Enable or disable RSTP protocol on the ports that are selected and set path cost.

RSTP Port Status

Port/Group	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1					Non-STP
Port 2					Non-STP
Port 3					Non-STP
Port 4	200000	no	yes	RSTP	Forwarding
Port 5	20000	no	yes	RSTP	Blocked
Port 6					Non-STP
Port 7					Non-STP
Port 8					Non-STP
Port 9					Non-STP
Port 10	200000	no	yes	RSTP	Forwarding
Port 11					Non-STP
Port 12	100000	no	yes	STP	Forwarding
Port 13					Non-STP
Port 14					Disabled
Port 15					Disabled
Port 16					Non-STP
Port 17					Non-STP
Port 18					Non-STP
Port 19					Non-STP
Port 20					Non-STP
Port 21					Non-STP
Port 22					Non-STP
Port 23					Non-STP
Port 24					Non-STP

Fig. 3-25 RSTP Port Status

Parameter description

Port / Group:

The RSTP information is listed per port or trunk

Path Cost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost, user can select auto or set the range from 1 to 200000000.

Edge:

Indicates whether this port is configured as edge port

P2P:

Informs if this port is connected as point to point link

Protocol:

Shows the used protocol

State:

Shows the port state (forwarding, blocking, learning or non-stp this function is disabled)

3-3-5. IGMP Status

Function name

IGMP Status

Function description

Display IGMP status. In Fig. 4-22, the window shows VLAN ID for each multicast group.

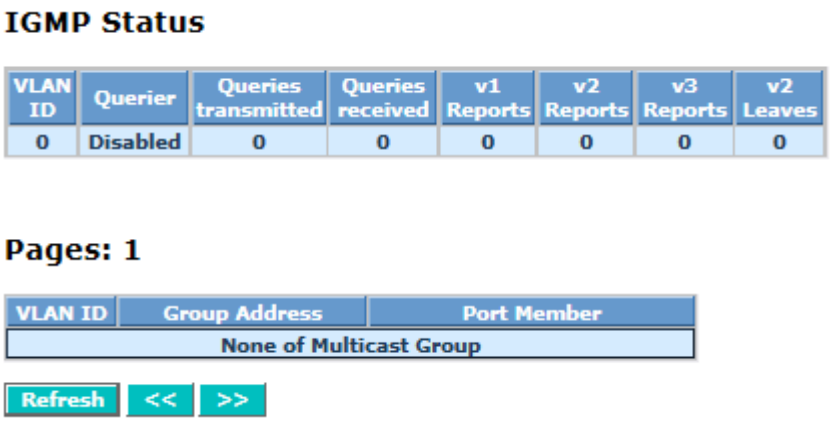


Fig. 3-26 IGMP Status

Parameter description

VLAN Id:

Show VLAN Id for each multicast group.

Querier:

Show the group membership queries status.

Queries transmitted:

To count the group membership queries transmitted.

Queries received:

To count the group membership queries received.

V1 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It calculates the number of times of IGMPV1 report.

V2 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV2 report.

V3 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV3 report.

V2 Leaves:

When a host leaves a group, it sends a leave group membership message to multicast routers on the network, it show the leaves number.

3-3-6. PoE Status

Function name

PoE State

Function description

Display the information about the PoE status.

PoE (Power over Ethernet) Status

Power Reservation	0%	0 W / 370 W

Port	PD Class	Power [W]	Current [mA]	Priority	Port Status
1	0	0	0	Low	NO_PD_DETECTED
2	0	0	0	Low	NO_PD_DETECTED
3	0	0	0	Low	NO_PD_DETECTED
4	0	0	0	Low	NO_PD_DETECTED
5	0	0	0	Low	NO_PD_DETECTED
6	0	0	0	Low	NO_PD_DETECTED
7	0	0	0	Low	NO_PD_DETECTED
8	0	0	0	Low	NO_PD_DETECTED
9	0	0	0	Low	NO_PD_DETECTED
10	0	0	0	Low	NO_PD_DETECTED
11	0	0	0	Low	NO_PD_DETECTED
12	0	0	0	Low	NO_PD_DETECTED
13	0	0	0	Low	NO_PD_DETECTED
14	0	0	0	Low	NO_PD_DETECTED
15	0	0	0	Low	NO_PD_DETECTED
16	0	0	0	Low	NO_PD_DETECTED
17	0	0	0	Low	NO_PD_DETECTED
18	0	0	0	Low	NO_PD_DETECTED
19	0	0	0	Low	NO_PD_DETECTED
20	0	0	0	Low	NO_PD_DETECTED
21	0	0	0	Low	NO_PD_DETECTED
22	0	0	0	Low	NO_PD_DETECTED
23	0	0	0	Low	NO_PD_DETECTED
24	0	0	0	Low	NO_PD_DETECTED
Total		0	0		

Refresh

Fig. 3-27

Parameter description

Power Reservation:

The watts are supplied by the PoE. The maximal power that the switch can supply (read only).

Port No:

Port number

PD Class:

Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.

Five classes are defined:

Class 0: Max. power 15.4 W

Class 1: Max. power 4.0 W

Class 2: Max. power 7.0 W

Class 3: Max. power 15.4 W

Class 4: Max. power 30.0 W

Power:

This entry shows how much power the PD currently is using.

Current

This entry shows how much current the PD currently is using.

Priority

The priority shows the port's priority configured by the user.

Port Status

This entry shows the port's status as following:

PoE not available - No PoE chip found - PoE not supported for the port.

PoE turned OFF - PoE disabled: PoE is disabled by user.

PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.

No PD detected - No PD detected for the port.

PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.

PoE turned OFF - PD is off.

Invalid PD - PD detected, but is not working correctly.

Total:

The sum of the current that every port supplies.

3-3-7. Ping Status

Function name

Ping Status

Function description

To set up target IP address for ping function and display ping status. In Fig. 4-24, the window shows the ping information.

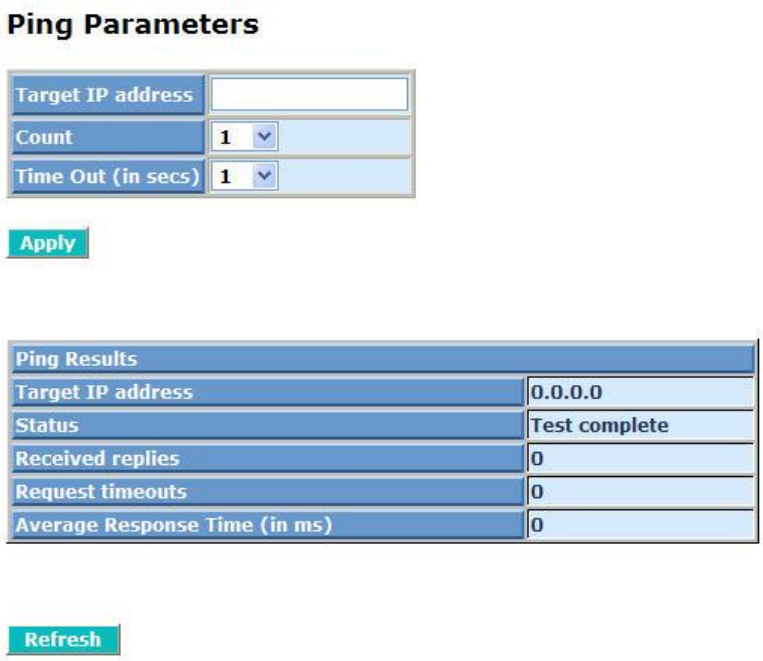


Fig. 3-28 Ping

Parameter description

Ping Parameters:

Target IP address:

Set up a Target IP address to ping.

Count:

Use drop-down menu to set number of echo requests to send. Four type of number can be chosen; there are 1, 5, 10 and 20.

Default: 1

Time Out (in secs):

Use drop-down menu to set number of echo requests time out in second. Four type numbers can be chosen; there are 1,5,10 and 20.

Default: 1

NOTE: All the functions should press **<Apply>** button to start up after you set up the parameters.

Ping Results:

Target IP address:

Show the active target IP address.

Status:

Show the result of the ping status.

Received replies:

Show the received replies number of times.

Request timeouts:

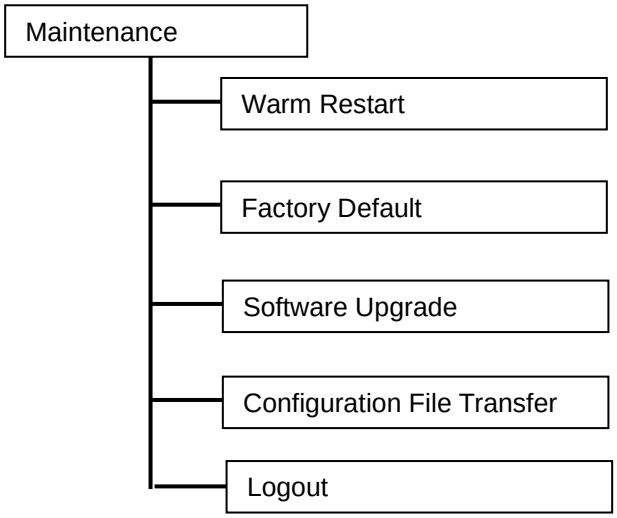
Show the timeout of request.

Average Response times (In ms):

Shows the average response time in milliseconds

3-4. Maintenance

There are five functions contained in the maintenance function.



3-4-1. Warm Restart

Web Smart Switch offers many approaches to reboot your switch, such as: power up, hardware reset and software reset. You can press RESET button in the front panel of your switch to reset the device and to retrieve default settings. After upgrading software, you have to reboot the device to have new configuration take effect. The function being discussed here is software reset.

Function name

Warm Restart

Function description

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. Press **<Yes>** button to confirm warm restart function and it will take around thirty (30) seconds to complete the system boot.

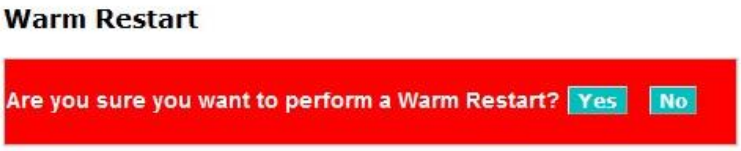


Fig. 3-29 Warm Restart

3-4-2. Factory Default

Function name

Factory Default

Function description

Factory Default provides the function to retrieve default settings and replace current configuration. Except the IP address setting, all settings will be restored to the factory default values when "Factory Default" function is performed. If you want to restore all configurations including the IP address setting to the factory default, please press the "RESET" button on the front panel.

Note for "RESET" button:

You must press the "RESET" button over 3 seconds to restore the factory default setting.

Fig. 3-30 Factory Default

3-4-3. Software Upgrade

Function name

Software Upgrade

Function description

You can just click Browse button to retrieve the file you want in your system to upgrade your switch.

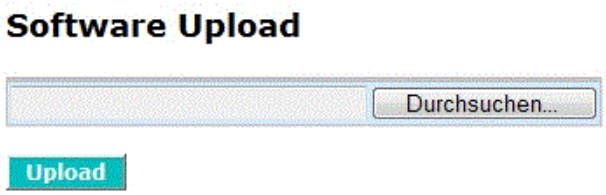


Fig. 3-31 Software Upgrade

3-4-4. Configuration File Transfer

Function name

Configuration File Transfer

Function description

You can backup your switch's configuration file into your computer folder in case accident happens. In addition, uploading backup configuration file into a new or a crashed switch can save much time and avoid mistakes.

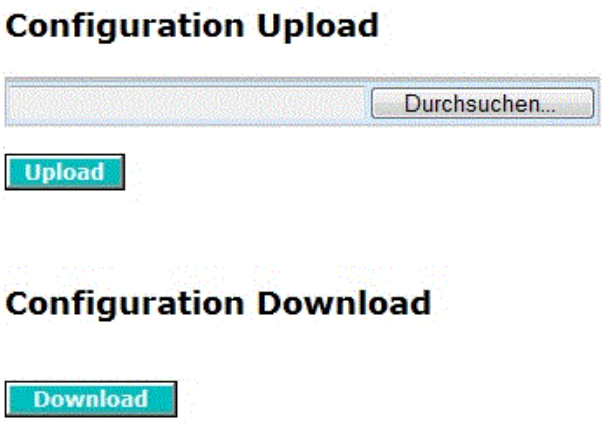


Fig. 3-32 Configuration Upload/Download

3-4-5. Logout

In addition to auto logout function we just mentioned in system configuration section, the switch also allows administrators to logout manually by Logout function.

Function name

Logout

Function description

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can set up the parameter of Auto Logout Timer in system configuration function to explicitly ON/OFF this logout function.

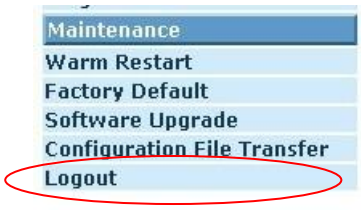


Fig. 3-33

Parameter description

Auto/Manual Logout:

If no action and no key is stroke as well in any function screen more than the minutes you set up in Auto Logout Timer, the switch will have you logout automatically. Or press the **<Logout>** button in Logout function to exit the system manually.

4. Maintenance

4-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty
- Mismatch of Auto-Negotiation settings

4-2. Q&A

1. Computer A can connect to computer B, but cannot connect to computer C through this switch.

   ✓ The network device of computer C may fail to work. Please check the link/act status of computer C on the LED indicator. Try another network device on this connection.
   ✓ The network configuration of computer C may be something wrong. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.

   ✓ The connection ports on another must be connection ports. Please check if connection ports are used on that switch.
   ✓ Please check the uplink setup of the switch to verify the uplink function is enabled.

3. The console interface cannot appear on the console port connection.

   ✓ This switch has no console port.

4. How to configure the 24 Port Gigabit Ethernet PoE Switch.

   ✓ User can use IE browser program in window series of computer to control the web smart functions in the switch. First, choose any port of the switch and connect the device with your network. Then, use IE and type default IP address, 192.168.1.1. Finally, the login screen will appear at once.

5. Disclaimer

All information in this document is provided "as is" and subject to change without notice. MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose of damage. Any product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "MICROSENS" is a trademark of MICROSENS GmbH and Co. KG, "IEEE" is a trademark of the Institute of Electrical and Electronics Engineers, Inc. "Microsoft" and "Windows" are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

1814-sh MS400830M_MAN_EN_V1.44

Appendix A
Technical Specifications

Features

- 20 (10/100/1000Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE802.3, 802.3u, 802.3z and 802.3ab.
- 4 Gigabit TP/SFP fibers are dual media ports with auto detected function.
- Non-blocking store-and-forward shared-memory Web-Smart switched.
- Supports auto-negotiation for configuring speed, duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any ports can be in disable mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Web-based management provides the ability to completely manage the switch from any web browser.
- Supports RSTP / STP
- Supports Port-based VLAN and Tag-based (IEEE802.1Q) VLAN.
- Auto-aging with programmable inter-age time.
- Supports 802.1p Class of Service with 2-level priority queuing.
- Supports port trunking with flexible load distribution and failover function.
- Supports port sniffer function
- Programmable maximum Ethernet frame length of range from 1518 to 9600 bytes jumbo frame.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.

Hardware Specifications

- **Standard Compliance**

  IEEE802.3/802.3ab/802.3z/802.3u/802.3x

- **Network Interface**

Configuration	Mode	Connector	Port
10/100/1000Mbps Gigabit TP	NWay	TP (RJ-45)	1 - 20
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	21 - 24 (Option)
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	21 - 24 (Option)
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	21 - 24 (Option)

  *Port 21 - 24 are TP/SFP fiber dual media ports with auto detected function
  *Optional SFP modules support BiDi transceivers

- **Transmission Mode**

  10/100Mbps support full or half duplex
  1000Mbps support full duplex only

- **Transmission Speed**

  10/100/1000Mbps for TP
  100/1000Mbps for Fiber

- **Full Forwarding/Filtering Packet Rate: PPS (packets per second)**

Forwarding Rate	Speed
1,488,000PPS	1000Mbps
148,800PPS	100Mbps
14,880PPS	10Mbps

- **MAC Address and Self-learning**

  8K MAC address

- **Buffer Memory**

  Embedded 512 KB frame buffer

- **Flow Control**

  IEEE802.3x compliant for full duplex
  Backpressure flow control for half duplex

- **Cable and Maximum Length**

TP	Cat. 5 UTP cable, up to 100m
1000Base-SX	Up to 220/275/500/550m, which depends on Multi-Mode Fiber type
1000Base-LX	Single-Mode Fiber, Distance depends on used SFP

- **Diagnostic LED**

System LED: System, Link/Act*, Speed*, PoE*
(* shows port LED mode)
Per Port LED: Link/Act/Speed

- **Power Requirement**

Voltage: 100-240VAC
Frequency: 50-60Hz
Consumption: 34W (typ.) except PoE
435W (typ.) with GBE Links and full PoE on all ports
PoE max.: 370W

- **Ambient Temperature:** 0-40° C
- **Humidity:** 10-90 % Relative Humidity
- **Dimensions:** 44(H)x442(W)x211.2(D)

Management Specifications

System Configuration	Auto-negotiation support on 10/100/1000Base-TX ports, Web browser can set transmission speed (10/100/1000Mbps) and operation mode (Full/Half duplex) on each port, enable / disable any port, set VLAN group, set Trunk Connection.
RSTP / STP Function	(Rapid) Spanning Tree
VLAN Function	Port-Base / 802.1Q-Tagged, allowed up to 24 active VLANs in one switch.
Trunk Function	Ports trunk connections allowed
Quality of Service (QoS)	Referred as Class of Service (CoS) by the IEEE 802.1P standard; Two queues per port
Network Management	Web browser support based on HTTP Server

Note: Any specification is subject to change without notice.